

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
9 December 2004 (09.12.2004)

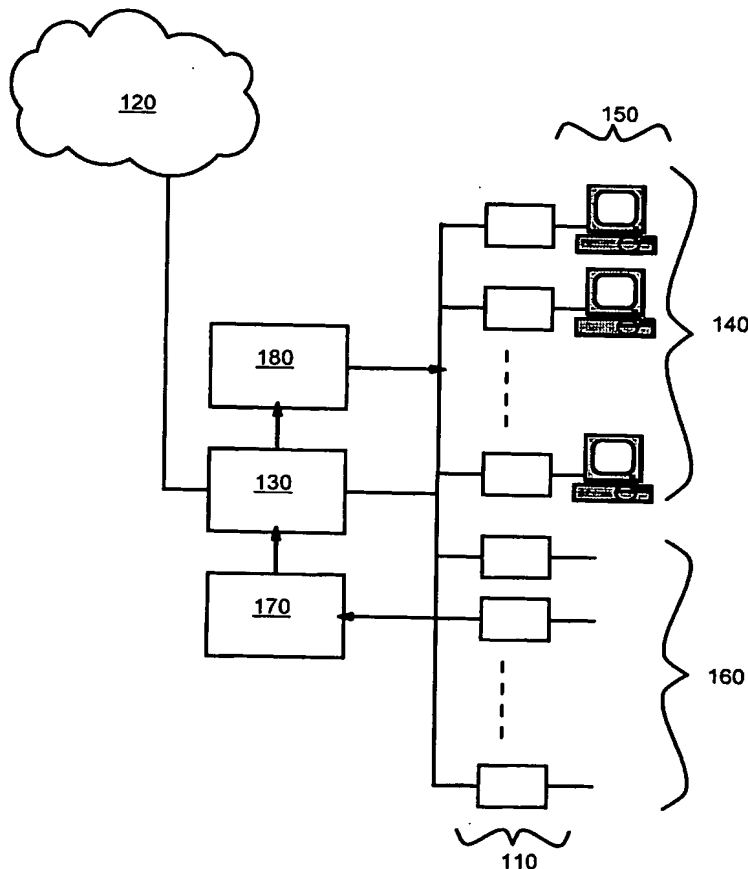
PCT

(10) International Publication Number
WO 2004/107706 A1

- (51) International Patent Classification⁷: **H04L 29/06, G06F 1/00**
- (21) International Application Number: **PCT/IB2003/005328**
- (22) International Filing Date:
20 November 2003 (20.11.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
03405393.4 30 May 2003 (30.05.2003) EP
- (71) Applicant (for all designated States except US): **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).
- (72) Inventor; and
(75) Inventor/Applicant (for US only): **RIORDAN, James, F.** [US/CH]; Alte Landstrasse 50, CH-8803 Rueschlikon (CH).
- (74) Agent: **KLETT, Peter, M.**; International Business Machines Corporation, Saeumerstrasse 4 / Postfach, CH-8803 Rueschlikon (CH).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: DETECTING NETWORK ATTACKS



(57) Abstract: Described is a technique for detecting attacks on a data communications network having a plurality of addresses for assignment to data processing systems in the network. The technique involves identifying data traffic on the network originating at any assigned address and addressed to any unassigned address. Any data traffic so identified is inspected for data indicative of an attack. On detection of data indicative of an attack, an alert signal is generated.



Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE,
SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA,
GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*